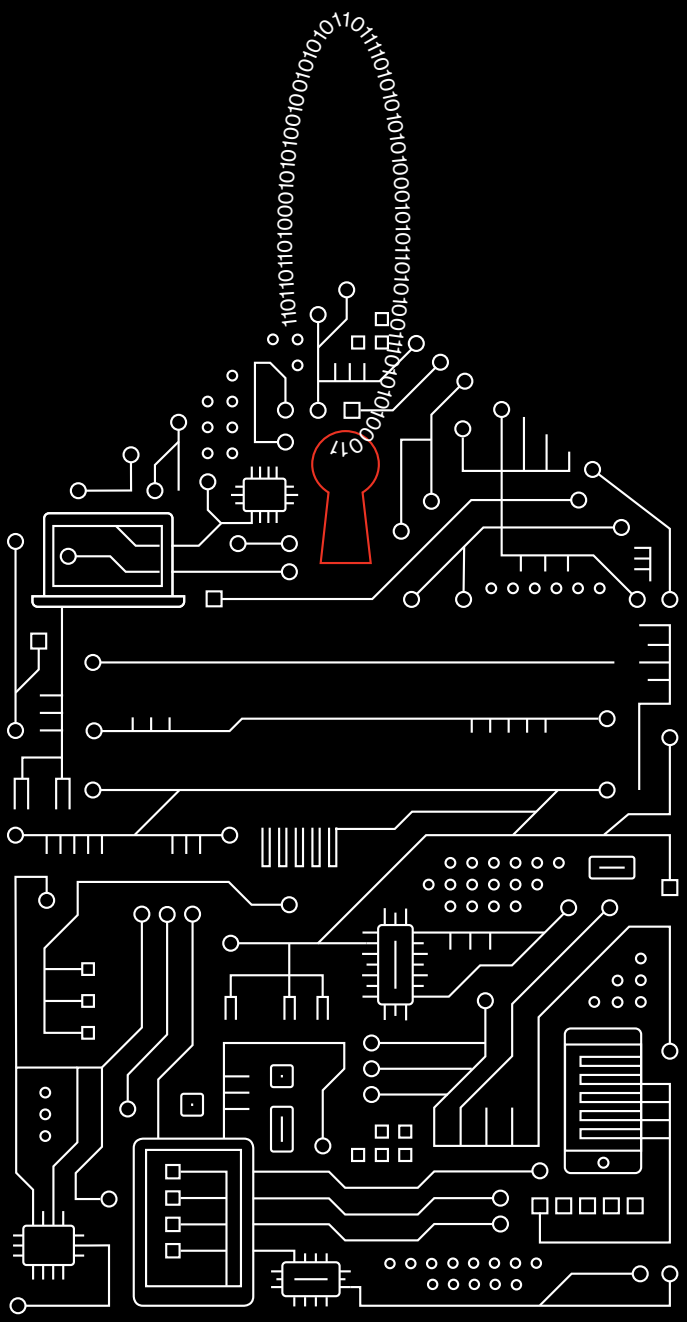
Mobile Security Index 2020

小売業界におけるモバイルセキュリティの現状

小売、旅行、サービス業界における
モバイルセキュリティの現状を詳細に分析



verizon

モバイルデバイスが原因で顧客のデータやロイヤリティにリスクが生じていませんか

サイバーセキュリティはもはやIT部門だけが考慮すべき問題ではありません。プライバシーやデータの保護に関する話題が繰り返しニュースで取り上げられるようになっており、また、小売業界の企業では、定期的にこれらのことが議題になっています。

83%

83%の小売業者が、モバイルデバイスは組織の円滑な運営に不可欠であると回答しています。

モバイルデバイスの強力な処理能力と多彩な機能は、小売業界の企業が現代の顧客に訴求し、物理的な店舗の魅力を維持するうえで大いに役立っています。一部の企業は、モバイルデバイスをクラウドベースのサービスと組み合わせて競争力を高め、差別化を図っています。特に小規模の企業ではこれが顕著であり、これら企業の83%は、大企業と伍していくうえでクラウドが大きな武器になっていると述べています。

しかし、カスタマーエクスペリエンスの質を高め、効率を向上させるためにモバイルテクノロジーを使い続けていくなかで、多くの企業では、データのセキュリティの確保に向けて対策を強化していく必要があるでしょう。

ベライゾンは独立系の調査会社に依頼し、モバイルデバイスの調達、管理、セキュリティを担当するシニアプロフェッショナルにアンケート調査を実施しました。合計876人の回答者のうち、小売業界の回答者は8%を超える割合を占めています。この数字のなかには、この業界のあらゆる規模の企業が含まれています。特に断りのない限り、本レポートのデータは、このアンケート調査によるものです。

verizon

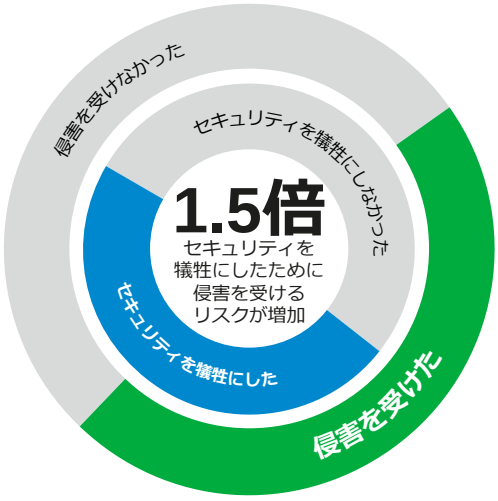
約30%の組織が侵害を受けている

小売業界の約3分の1（30%）の企業が、モバイルデバイスに関係した侵害を昨年受けたと認めています。侵害を受けた結果、業績やブランドイメージに影響が生じた企業に関する情報が数多くありますが、この数字は前回の調査のときとほぼ変わっていません。

大小を問わず、ニッチ市場の企業も有名企業も含め、小売業界ではあらゆる規模の企業が侵害を受けています。米国のレストランチェーンの親会社はマルウェアベースの攻撃に遭い、200万のクレジットカード情報が流出しました[1]。欧州の大手航空会社が受けた侵害では、50万人の顧客の個人情報が盗まれています[2]。ベライゾンの調査によれば、中小企業（SMB）の28%がモバイルデバイス関連のセキュリティ侵害に遭っていることが判明しています。

87%

87%の企業がモバイルセキュリティ侵害により長期に亘って顧客ロイヤリティに大きな影響が生じるのではないかという懸念を示しています。



40%

40%の企業がセキュリティを犠牲にしたことがあると回答しています。

30%

41%の企業がセキュリティ侵害を受けたことがあると認めています。

図1：モバイルデバイスやIoTデバイスに関連したセキュリティ侵害を昨年受けた企業の割合。業務を遂行するためにIoTデバイスを含むモバイルデバイスのセキュリティを犠牲にした割合。

顧客ロイヤリティやブランド価値がダメージを受ける恐れがあるに関わらず、40%の企業が「業務を遂行」するためにモバイルセキュリティを犠牲にしたと認めています。他の業界と同様に、その結果は明らかです。セキュリティを犠牲にしたと述べた企業は、そうでない企業と比較して1.5倍侵害を受けるリスクが高くなっています。

小売業の在り方を変革

モバイルテクノロジーは小売業の分野で重要な役割を果たしていることは明白です。この業界ではこのテクノロジーを活用して、オンラインサービスと実店舗が提供する実体のあるエクスペリエンスを組み合わせ、カスタマーエクスペリエンスを変革しています。店舗では、セルフサービスのキオスクやモバイルPOSなどのイノベーションにより利便性が向上しており、接客の質を高められるようになっています。また、サプライチェーンにおけるコスト管理が容易になり、無駄を削減しつつ在庫管理も効率化されています。

小売業界では、モバイルデバイスを様々なかたちで利用していますが、これらはクラウドにより実現されています。アプリを開発、実行する場合、ほとんどのケースにおいてまずはクラウドが選択されます。新たに作成したビジネス情報の半分以上をクラウドに保管していると、62%の企業が回答しています。

ほとんどの小売事業者が、自社の組織内で使用されているアプリの数を著しく少なめに計算しており、その数は100未満である半数の企業が回答しています。1,000を超えるアプリを使用していると回答した企業はわずか11%でした。しかし実際の平均数は、もっと大きな数字になっています。

1,300

Netskopeによれば、組織では平均で約1,300のアプリとクラウドサービスが利用していますが、そのうちの95%が管理されていない状態にあり、IT部門はこれらアプリやサービスに対する管理権限を持たず、その状態を把握すらしていません[3]。

80%

80%の企業が、今後5年以内にモバイルがクラウドサービスにアクセスするための主要な手段になると回答しています。

33%

3分の1（33%）の小売業者が、自社のブランド名を悪用した不正なホットスポットの存在を確認していると回答しています。ハッカーはこれらのホットスポットを使い、ユーザーが閲覧しているサイトを盗み見たり、認証情報を傍受したり、デバイスにマルウェアを侵入させたりしています。

小売業者が大きな脅威と考えるモバイルセキュリティ上の問題

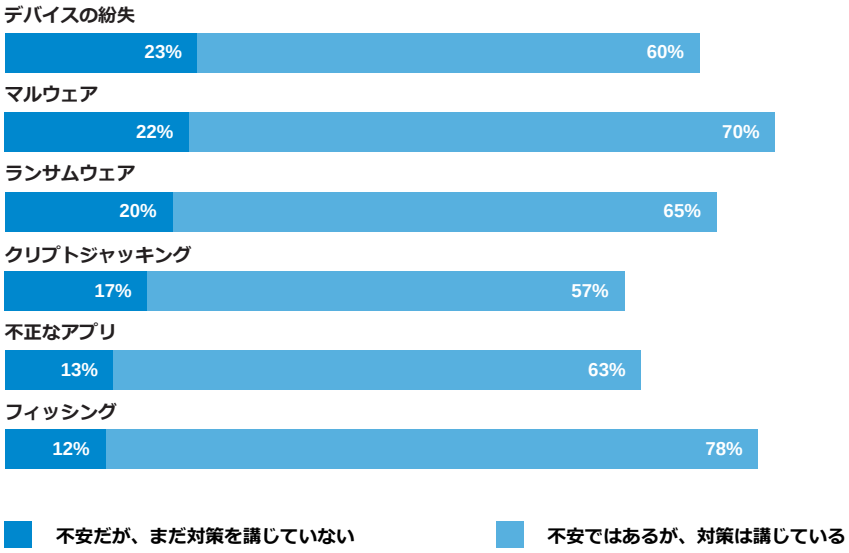


図2：脅威や脆弱性の問題をどう捉えているか

既知の脅威

小売業界はモバイルデバイスを狙う脅威に懸念を示しており、77%がそのビジネスリスクの高さを「中」から「高」と位置付けています。また、「クリプトジャッキング」をはじめとする新たな脅威も含め、様々な脅威の存在が気がかりであると述べています。しかし、対応の準備ができていないと感じている脅威は多くの場合既知であり、特によく挙げられるものは、デバイスの紛失や盗難に起因する脅威（23%）やマルウェア（22%）、ランサムウェア（20%）があります。

サプライチェーンに生じる業務の停止や遅延を心配する回答がある一方、顧客のデータが窃取されることを懸念する回答者はもっと多く、その割合は71%になっています。そしてさらに多くの回答者（74%）が、従業員のデータに対する侵害に不安を抱いていると述べています。このデータは、税金などに関連する高度に標的を絞ったフィッシング詐欺の主要な標的になっています。

悪意のない脅威

近年大きな注目を集めている脅威として「内部の脅威」があります。78%の企業が、自社の従業員がモバイルデバイスに関する最大のリスクであると回答しています。

不注意によるものであっても、従業員の行動が企業を大きな危険にさらす恐れがあるのは間違いありません。許可されていないアプリのインストールや安全でない公衆Wi-Fiのホットスポットへの接続など、その行動の種類は様々です。そしてこの問題は、派遣社員や契約社員の採用に伴い、さらに深刻化することが少なくありません。しかしあまりに多くの企業がリスクを意識していながらセキュリティを犠牲にしており、モバイルポリシーの設定担当者自らがルールを破っているのが現状です。このような状況で従業員に適正な行動を期待するのは筋違いであり、果たして、適切なリスク管理と言えるでしょうか。

88%が現場のスタッフはモバイルデバイスを使用していると回答している一方、これらの従業員が高いセキュリティ意識を持っていると回答したのはわずか37%でした。そして、たった45%の企業がスタッフに対して継続的なセキュリティトレーニングを実施していると回答しています。

小売業界のセキュリティ対策には改善の余地がある

大きなリスクが存在するにもかかわらず、小売業者の多くは基本的な予防措置を講じていません。デフォルトのパスワードやベンダー提供のパスワードを全て変更していると回答した企業は、半数未満（47%）にとどまっています。また、公衆ネットワークで機密データを送信する際にデータを暗号化していると回答したのは43%しかいません。これらの2つは、定期的なセキュリティテストや、データアクセスの権限を必要最小限に限定する措置と同様、極めて基本的なセキュリティ対策に位置付けられるものです。これら4つの基本的な予防措置を全て実施している企業はわずか17%にすぎません。

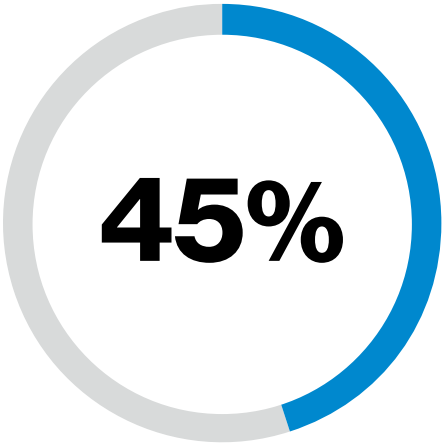
そして、クラウドの利用が増加しているにも関わらず、小売業界の18%の組織が、クラウドベースのサービスに関して特別のセキュリティ対策を講じていないと述べており、セキュリティ強度を事前検証することなくクラウドアプリを使用しないよう制限をしていると回答した企業は、わずか40%にとどまっています。そして、未知のネットワークやロケーションからアクセスがあったときにクラウドアプリの使用をブロックしたり、機能を制限したりしていると回答したのは、約半数（51%）しかいませんでした。このような基本的な予防措置を怠っていると、顧客や従業員、ビジネスデータが大きなリスクに晒される危険があります。

なぜ対応を誤ってしまうのか

セキュリティを犠牲にしてしまう理由として、収益目標達成の圧力（54%）、利便性（54%）、便宜的な理由（46%）が上位３つに挙げられています。つまり、流通・小売、旅行、サービス事業者のセキュリティ対策を妨げているのは、予算上の問題だけではなく、セキュリティ対策が生産性や効率に及ぼす影響を意思決定者が懸念していることも関係しているのです。セキュリティポリシーの設計や導入に問題があると、従業員のエクスペリエンスや企業のパフォーマンスに悪影響を及ぼすことになります。パスワードポリシーのような単純なものでも、従業員の生産性の低下につながる恐れがあります。再テストが増えれば、サポートの費用が増える可能性もあります。従業員がルールの抜け道を利用するようになるとリスクが増大する危険も生じます。

70%

70%が公衆Wi-Fiを個人的に業務に利用していると回答しており、このうち31%の企業ではそれがポリシーで明確に禁じられているにも関わらず利用されていました。



約半数（45%）の企業が、予算不足によりモバイルデバイスのセキュリティを強化する取り組みが妨げられていると回答しています。

IoTで脅威は増すのか

ワイヤレス接続するデバイスの数や種類が大幅に増加しており、スマートIoTデバイスが小売業界のビジネスに変革をもたらしています。そして、67%が、IoTデバイスはデ ジタルトランスフォーメーションに不可欠であると回答しています。

この業界では、IoTデバイスはデジタルサイネージなどの機能によるカスタマーエクスペリエンスの強化(67%)のほか、建物の物理的なセキュリティの強化(67%)、設備の稼働率や従業員の生産性の向上(60%)に利用されています

IoTによって生じる特定のセキュリティリスクの調査では、これらデバイスの調達や管理、セキュリティ担当者のグループに対してもインタビューを実施しましたが、回答者の87%が、自身の組織がIoTデバイスを標的にした攻撃のリスクに晒されていると回答しており、リスクの高さを「中」から「高」と位置付けています。そして47%が既にIoTデバイスに関連する侵害を受けていると回答しており、他のモバイルデバイスについても、50%を超える回答者が侵害を受けたと回答しています。

このようにIoTデバイスのセキュリティリスクが認識されているにも関わらず、33%が「業務を遂行」するためにそのデバイスのセキュリティを犠牲にしたと回答しています。なぜそうなってしまうのでしょうか。原因としては便宜的な理由が挙げられます。80%の回答者が、その決定の背後には時間的なプレッシャーがあると言います。競争に勝ち残るために、小売業界は革新的なカスタマーエクスペリエンスを実現しなければなりません。競合他社と同等か、より優れたエクスペリエンスを創出する必要があります。しかし多くの場合、市場にいち早く商品やサービスを投入しようとするあまり、セキュリティを二の次にしてしまうのです。そして、27%が、IoTデバイスのセキュリティを最優先として考えるべきものではなく「後回し」にできると回答しています。

47%

47% が IoT デバイス関連のリスクが過去 1 年で増加したと考えていると回答しています。

67%

67%が全社的に展開しているIoTデバイスが少なくとも1種類はあると回答しています。

IoTデバイスを安全に利用する

IoTのセキュリティを強化する方法は数多くあります。全モバイルデバイスを対象に弊社のアドバイスに従って対処を行い、以下に示すIoT固有の4つのベストプラクティスを実行すれば、セキュリティを確保できます。

1.ソリューションやコンポーネントを購入する前に、そのセキュリティをチェックする
市販のソリューションを購入する場合であれ、既成のコンポーネントを調達して独自のIoTデバイスを構築する場合であれ、ソリューションやコンポーネントの提供元のベンダーにベンダーのセキュリティ対策の詳細を確認し、セキュリティの強度をチェックします。認証や暗号化の機能、パッチのポリシーについては特に重点的に確認します。76%が、IoTデバイスをリモートで使用している、またはアクセスが難しい場所に設置していると回答していますが、そのような場合は、無線通信（OTA）でアップデートをすれば、デバイスをセキュアな状態に維持できます。

2.ネットワークに接続するデバイスのセキュリティを事前に強化する
まずはデバイス自体に改竄防止機能や改善検出機能があることを確認します。次に、デフォルトのパスワードやベンダー提供のパスワードを全て変更します。また、必要のない機能などは無効にして、極力ハッカーに隙を見せないようにします。使用していないポートやプロトコルがあればブロックします。

3.移動する時も保存する時もデータを暗号化する
83%の回答者が個人情報（PII）を収集していると回答していますが、このうちの25%がそのデータを暗号化していませんでした。データを暗号化すれば、ハッカーはそのデータを悪用できなくなるため、ブランドイメージの失墜につながるデータ侵害のリスクを抑えることができます。

4.IoTプラットフォームを使用する
すべてのデバイスを簡単に監視および管理できるIoTプラットフォームを選択します。このプラットフォームでは、デジタル証明書などのセキュリティ機能を実装して、脆弱性を減らすことができます。また、IoTプラットフォームはSIMをデバイスにバインドするため、SIMが盗難にあった際の被害を抑えてサイバー攻撃の影響を緩和できます。

78%

78%がIoTデバイスに関連したリスクが新たな脆弱性によって今後増加すると予想しています。

verizon

攻撃を受ける前に行動しなければならない

侵害に遭った小売業者の61%が、過去1年でモバイルセキュリティへの投資が大幅に増加したと回答しており、また、侵害を受けた56%が、今後1年でモバイルセキュリティの投資を大幅に増やすと回答しています。一方、侵害に遭っていない場合、割合はそれぞれ、わずか19%と17%になっています。

90%

90%がモバイルデバイスのセキュリティをもっと真剣に考える必要があると回答しています。

モバイルセキュリティの問題を是正しようとする動きが企業に見られるのは良い傾向です。しかし、被害を受けるまで行動を起こさない企業があまりに多い点は気がかりです。

このような状況では、モバイルに関連したセキュリティ攻撃が発生した場合その影響は深刻なものとなり、影響が長引くことになります。侵害に遭った61%の企業が、復旧作業は困難をきたし多額の費用がかかったと回答しています。

侵害を受けたことに気付いてからモバイルセキュリティを見直すのではなく、今こそ行動を起こさねばなりません。

次のステップ

MSI 2020のメインレポート
完全版のMobile Security Index 2020レポートには、モバイルデバイスが直面している脅威についてのさらに詳細な統計情報と分析が記載されています。FBIの主任捜査官やベライゾンの最高情報セキュリティ責任者（CISO）をはじめとするセキュリティエキスパートへのインタビューも掲載しています。

MSI 2020のセキュリティ評価ツール
ベライゾンのモバイルセキュリティ評価ツールでは、MSI 2020レポートのデータとお客様のセキュリティの状況を理解、リスクの認知、リスクの度合い、備えの4分野で比較して、カスタムレポートを作成できます。レポートにはお客様のセキュリティを強化するための指針が記載されます。

MSI 2020の利用規定ガイド
このインタラクティブガイドでは、強固なAUPを構成する要素についてご説明するとともに、お客様がご自身でAUPの作成と改善し、マルウェアやフィッシングなどのリスクを軽減するためのヒントをご紹介しています。

アドバイス

ユーザー

- 正式なAUPを定め、個人所有デバイスの業務利用に関する責任や使用できるネットワーク、ユーザーがインストールできるアプリを規定
- セキュリティファーストの視点に重点を置き、すべての従業員に定期的なトレーニングを施し、疑わしい事象を報告するための手順を周知
- パスワードの強度や再利用、2要素認証について規定したパスワードのポリシーを定めて周知

アプリ

- データアクセスの権限を必要最小限に限定
- 従業員がインストールできるアプリを出所の明確なソースから入手したアプリのみに制限し、インターネットからダウンロードしたアプリはブロック
- すべてのパッチを迅速にインストール

デバイス

- ベンダーから提供されたデフォルトのパスワードをすべて変更し、同じパスワードを再利用しない
- 脆弱性のあるデバイスやマルウェアに感染したデバイス、紛失したデバイスや盗まれたデバイスを対象としてデバイスのロックダウンや隔離を行うよう、各種のポリシーを導入
- モバイルデバイス管理（MDM）ソリューションにより、パッチの管理を簡素化し、認証ポリシーなどのAUPを適用
- モバイル上の脅威を検知するソフトウェアを導入し、デバイスを定期的にスキャンして脆弱性の有無を確認

ネットワーク

- セキュアでないネットワークを介して送信するデータはすべて暗号化
- 公衆Wi-Fiの危険性をユーザーに周知し、未知のWi-Fiネットワークや安全でないWi-Fiネットワークの使用をブロック
- ゼロトラストアプローチの採用を検討

クラウドサービス

- 特にファイル共有アプリなどで、出所の怪しいクラウドアプリの使用を制限
- 信頼できるネットワークやVPNを使用しているデバイスのみにクラウドサービスへのアクセスを許可

詳細は、enterprise.verizon.com/msiをご覧ください。

Verizon Mobile Security Index について

本年の報告が第3版となるMobile Security Indexは、モバイルのセキュリティに関する主要な情報ソースの1つとなっています。本年のMSIでは、独立の調査機関に委託し、組織においてモバイルデバイスとIoTデバイスの調達、管理、セキュリティを担当している876人のプロフェッショナルに調査を実施しました。このレポートでは、Asavie、IBM、Lookout、MobileIron、NetMotion、Netskope、Symantec、VMware、Wanderaといったモバイルデバイスのセキュリティ分野を牽引する企業の協力も得ながら、さらに詳しい調査を実施しており、これらの企業からはインシデントやデバイスの利用状況に関する追加情報をご提供いただきました。さらに今回は、FBIと米国のシークレットサービスからも協力が得られました。モバイルデバイスを脅かす脅威の全容とその対策を明らかにするうえで、皆様には多大なご尽力をいただきました。厚く御礼申し上げます。

verizon✓

1 Komando.com、「The biggest security breaches of 2019, so far」、2019年8月8日
2 BBC、「British Airways faces record £183m fine for data breach」、2019年7月8日
3 Netskope、『Netskope Cloud Report』（https://resources.netskope.com/cloud-reports/netskope-cloud-report-august-2019）、2019年8月